REMARKS

Reconsideration and allowance are requested.

Claims 2 and 8 stand rejected under 35 U.S.C. §101 for alleged inoperativeness and lack of utility. Amended claim 2 describes "a new value Rd_I given by [(inverse (X_I XOR Y_I)) XOR (a value of Rd_I currently stored in one of said three further registers)]." Support for this amendment is found for example in Figure 11 and page 13, lines 10-13. Rd[i]t in Figure 11 represents the value currently stored in one of the three further registers, and Rd[i]t+1 is the new value of Rd. Similarly, claim 5 is amended to recite "a new value Rd_I given by [(inverse (X_I XOR Y_I)) XOR (a value of Rd_I currently stored in one of said shared dummy registers)]." Claims 8 and 11 are similarly amended. These amendments provide the clarification requested by the Examiner. Withdrawal of this rejection is requested.

Applicants appreciate the indication of allowable subject matter in claims 2, 4-6, 8, and 10-12. Claims 1, 3, 7, and 9 stand rejected under 35 U.S.C. §103 for obviousness based on Pomet. This rejection is respectfully traversed.

In response to the claim interpretation outlined in the final office action, amended claims 1 and 8 to describe that the register write circuit is configured to also write data values to three of more further registers such that "the number of bits within said data processing register and said three or more further registers as a whole that transition from high to low equals the number of bits within said data processing register and said three or more further registers as a whole that transition from low to high." Support for this amendment is found for example on page 13, lines 20-21: "a balanced equal number of transitions from high to low and low to high" and in Figure 11, where there are an equal number of high-low transitions and low-high transitions.

Pomet does not ensure that the number of bits which change from high to low equals the number of bits that change from low to high, and thus, Pomet lacks the quoted claim feature. In the system of Pomet, "there will always be a switching of two of the loops of the secured D type master-slave flip-flop circuit according to the invention" (column 6, lines 9-1 1). Thus, Pomet just ensures that the number of loops (or bits) switching is fixed—not that the number of bits switching from high to low equals the number of bits switching from low to high.

The Examiner seems to acknowledge this in paragraph 12 of the Office Action: "...the total number of transitions must be fixed. As pointed out by the applicant, this is exactly what Pomet discloses." Indeed, Figure 3 of Pomet makes it clear that the number of bits changing from low to high does not equal the number of bits changing from high to low. Consider the first few clock cycles: at the rising edge of the first clock pulse, two loops change from low to high, and no loops change from high to low; at the trailing edge of the first clock pulse, two loops change from high to low, and no loops change from low to high; and at the rising edge of the second clock pulse, three loops change from low to high and none from high to low. Thus, it is clear that the number of high-low and number of low-high transitions are not equal.

The inventors in this application recognized that when a register write occurs there can be a difference in power consumed depending on how many bit values transition from high to low compared with how many bit values transition from low to high. By ensuring that the number of bits within the data processing register and three further registers as a whole that transition from high to low equal the number of bits that transition from low to high irrespective of the data value being written, externally visible characteristics that depend on the data value being written are masked, and the security of the system is improved.

The application is in condition for allowance. An early notice to that effect is earnestly solicited.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: _____
John R. Lastova
Reg. No. 33,149

JRL:maa
901 North Glebe Road, 11th Floor
Arlington, VA 22203-1808
Telephone: (703) 816-4000
Facsimile: (703) 816-4100